1. (Amended) A security system for a computer connected to a network of computers comprising:

at least one security subsystem associated with said computer, said subsystem being configured to correlate events across a plurality of devices associated with said network of computers and to detect attacks on said computer;

C1

and a securė link between said security subsystem and a master system enabling data communication therebetween; wherein

said master system monitors said security subsystem through said secure link and registers information pertaining to attacks detected by said security subsystem.

5. (Amended) A network security system for a target network of computers comprising:

at least one security subsystem associated with said target network, said subsystem being configured to correlate events across a plurality of devices associated with said target network of computers and to detect attacks on said network; and

C2

a secure link between said security subsystem and a master system enabling data communication therebetween; wherein

said master system monitors said security subsystem through said secure link and registers information pertaining to the attacks detected by said security subsystem.

8. (Amended) A network security system for a target network of computers comprising:

C3

at least one security subsystem associated with said target network and configured to correlate events across a plurality of devices associated with said target network and to detect and register attacks on said target network;

Received from < 1 212 705 1987 > at 3/26/03 3:21:24 PM [Eastern Standard Time]

a secure link for data communication between said security subsystem and said master system; and

C3

testing means associated with said master system for generating pseudo-attacks on said target network initiated by said master system and detectable by said security subsystem; wherein

said master system monitors said security subsystem through said secure link by comparing the pseudo-attacks generated by said testing means to the detected attacks registered by said security subsystem.

11 (Amended) A method for monitoring the integrity of a security subsystem associated with a target network of computers and configured to detect attacks on said network of computers comprising:

C4

correlating events across a plurality of devices associated with said target network using said security subsystem;

establishing a secure link for the transfer of data between said security subsystem and a master system hierarchically independent from said security subsystem;

monitoring the status of said security subsystem through said secure link; and

registering information pertaining to the status of said security subsystem.

13. (Amended) A security system for a computer connected to a computer network comprising:

C5

at least one detection means associated with said computer, said detection means being configured to correlate events across a plurality of devices associated with said computer network and to detect an attack on said computer;

a master security system located outside said computer network; and

C5

a secure link between said detection means and said master security system enabling data communication therebetween; wherein

said master security system monitors said detection means through said secure link and registers information pertaining to attacks detected by said detection means.

C6

17. (Amended) A network security system for a target network of computers comprising:

at least one detection means associated with said target network, said detection means being configured to correlate events across a plurality of devices associated with said computer network and to detect an attack on said network;

a master security system located outside said network; and

a secure link between said detection means and said master security system enabling data communication therebetween; wherein

said master security system monitors said detection means through said secure link and registers information pertaining to attacks detected by said detection means.

C7

21. (Amended) A method for monitoring the integrity of a detection means associated with a computer, said computer being connected to a computer network, and configured to detect an attack on said computer, said method comprising the steps of:

correlating events across a plurality of devices associated with said computer network using said detection means;

establishing a secure link for the transfer of data between said detection means and a master system hierarchically independent from said detection means;

monitoring the status of said detection means through said secure link; and